Central Depository Services (India) Limited

Convenient ⌖ Dependable ⌖ Secure

COMMUNIQUÉ TO DEPOSITORY PARTICIPANTS

CDSL/OPS/DP/POLCY/2025/27 **January 10, 2025**

IMMEDIATE CYBER INCIDENT & QUARTERLY CYBER INCIDENT REPORTING BY DPs

DPs are advised to refer to SEBI circular No: SEBI/HO/MIRSD/TPD/P/CIR/2022/93 dated June 30, 2022, wherein all Cyber-attacks, threats, cyber-incidents and breaches experienced by Stock brokers / Depositories Participants shall be reported to **Stock Exchanges / Depositories & SEBI within 6 hours of noticing / detecting** such incidents.

In view of the above, Depository Participants are hereby informed that CDSL has developed a facility for online submission of cyber incident reporting through audit web portal. Depository Participants shall also report about such incidents to CDSL through the dedicated e-mail id: **dpincident@cdslindia.com.**

For submitting the **immediate cyber incident report** to Stock Exchanges / Depositories, please refer **Annexure A.**

Further the incident shall also be reported to Indian Computer Emergency Response team (CERT-In) in accordance with the guidelines / directions issued by CERT-In from time to time. Additionally, the Stockbrokers / Depository Participants, whose systems have been identified as “Protected system” by National Critical Information Infrastructure Protection Centre (NCIIPC) shall also report the incident to NCIIPC.

In addition to this, Stock Brokers / Depository Participants **must submit mandatory quarterly reports** to Stock Exchanges / Depositories on cyber-attacks, threats, incidents, breaches, and mitigation measures, including useful information on vulnerabilities, **within 15 days after the end of each quarter** i.e. Apr-June **(Q1),** Jul-Sep **(Q2),** Oct-Dec **(Q3),** Jan-Mar **(Q4).**

For submitting the **quarterly cyber incident report** to Stock Exchanges / Depositories, please refer **Annexure B.**

Queries regarding this communiqué may be addressed to: CDSL – Helpdesk Emails may be sent to: dprtasupport@cdslindia.com and connect through our IVR Number 022-62343333.

For and on behalf of

Central Depository Services (India) Limited

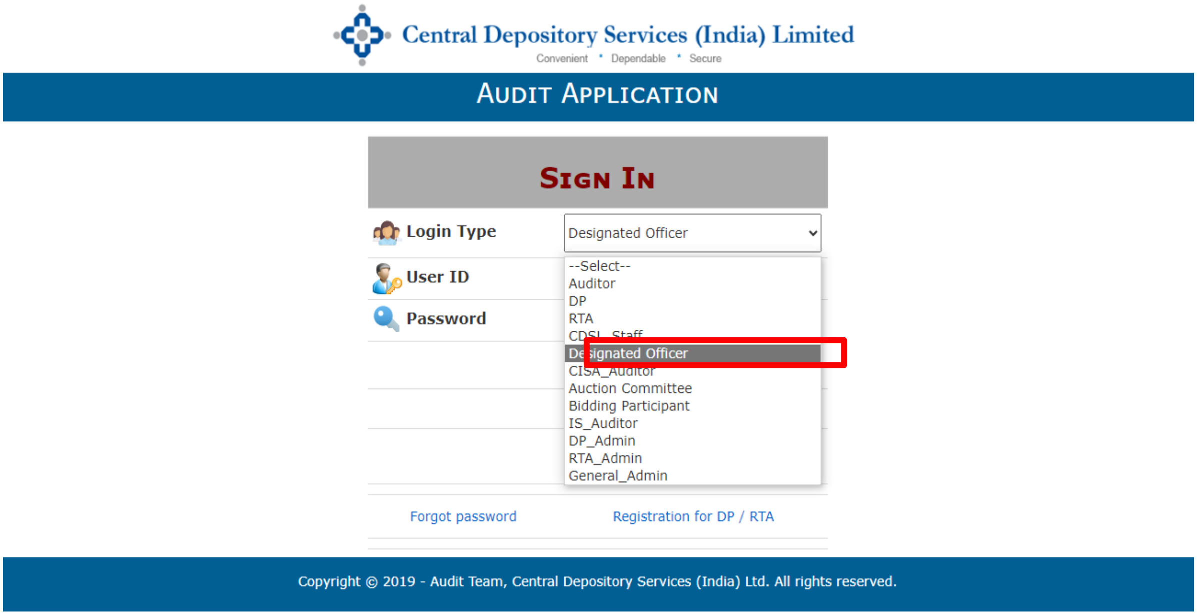
sd/-

Akhil Wadhavkar
Vice President– Information Technology

Annexure A

Guidelines to submit Immediate Cyber Incident Report

1. Open the Audit Web Portal.
   - Link: https://auditweb.cdslindia.com/Login.aspx
   - Click on Login Type and select "**Designated Officer**" login.



Central Depository Services (India) Limited

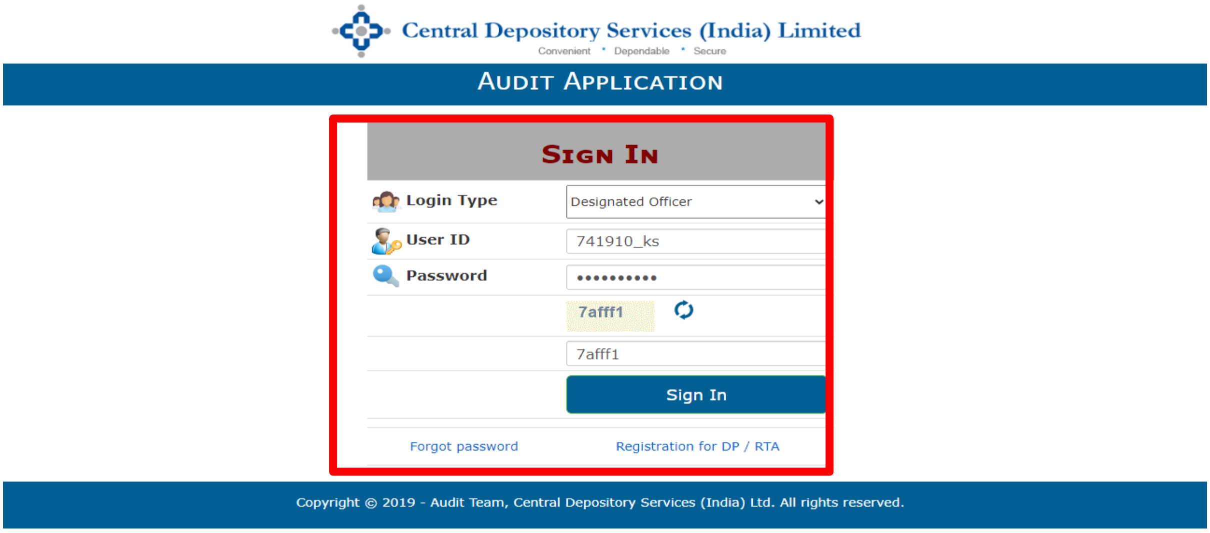
AUDIT APPLICATION

SIGN IN

Login Type: Designated Officer

Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.

2. Fill the below required information and click on "**Sign In**" Button:
   - User ID , Password & Captcha



Central Depository Services (India) Limited

AUDIT APPLICATION

SIGN IN

Login Type: Designated Officer

User ID: 741910_ks

Password: ••••••••••

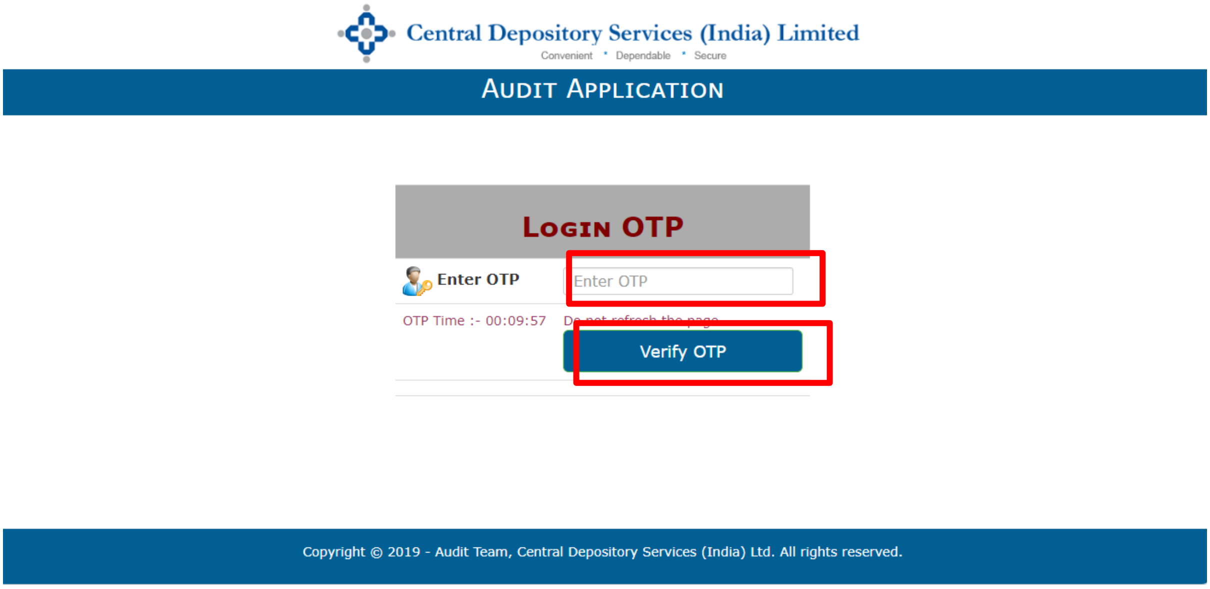
7afff1

7afff1

Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.

3. Enter the OTP:

- You will receive the OTP on both your DP's registered mobile number and email Id.



Central Depository Services (India) Limited

Convenient • Dependable • Secure

AUDIT APPLICATION

LOGIN OTP

Enter OTP: Enter OTP

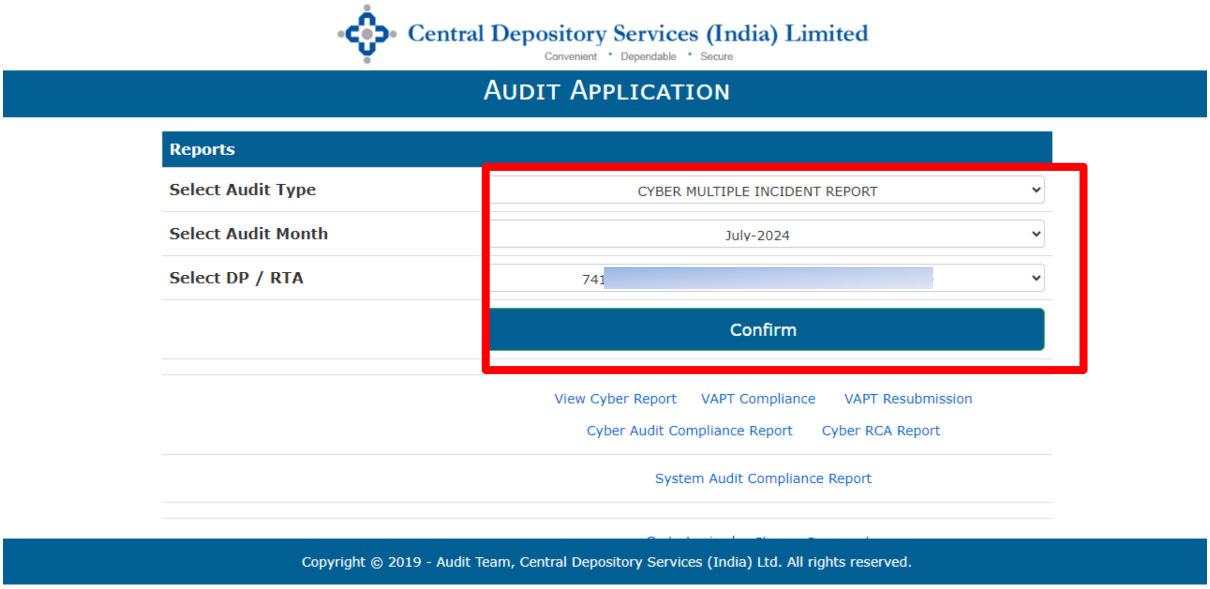
OTP Time :- 00:09:57 Do not refresh the page

Verify OTP

Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.

4. Select required information for submitting **immediate** "**Cyber Incident**" report:

- Select Audit Type: **CYBER MULTIPLE INCIDENT REPORT**
- Select Audit Month: **Select the current month**
- Select DP/RTA: **Select your DP ID**
- Click on the "**Confirm**" Button



Central Depository Services (India) Limited

Convenient • Dependable • Secure

AUDIT APPLICATION

Reports	
Select Audit Type	CYBER MULTIPLE INCIDENT REPORT
Select Audit Month	July-2024
Select DP / RTA	741[redacted]
	Confirm

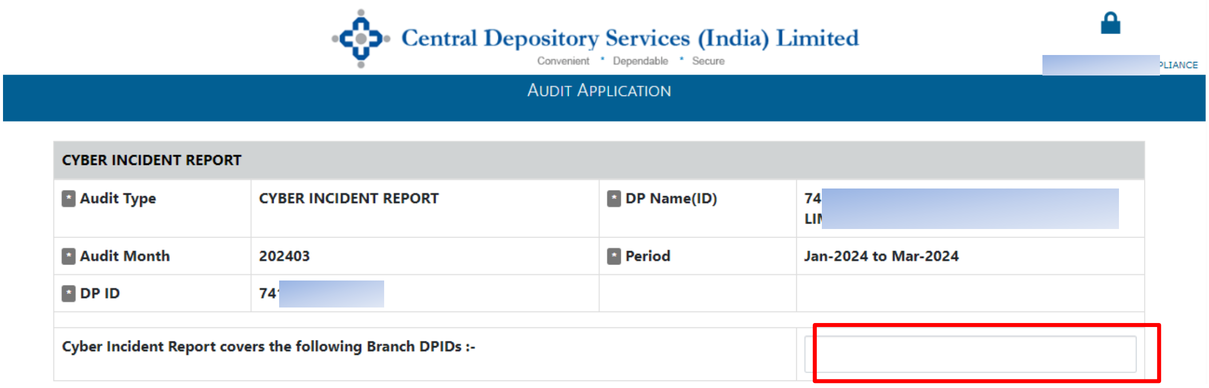
View Cyber Report   VAPT Compliance   VAPT Resubmission

Cyber Audit Compliance Report   Cyber RCA Report

System Audit Compliance Report

Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.

5. The following screen will appear. Main DP can mention the branch DP IDs, if they are submitting consolidated report for branch DP IDs.



Central Depository Services (India) Limited
Convenient • Dependable • Secure

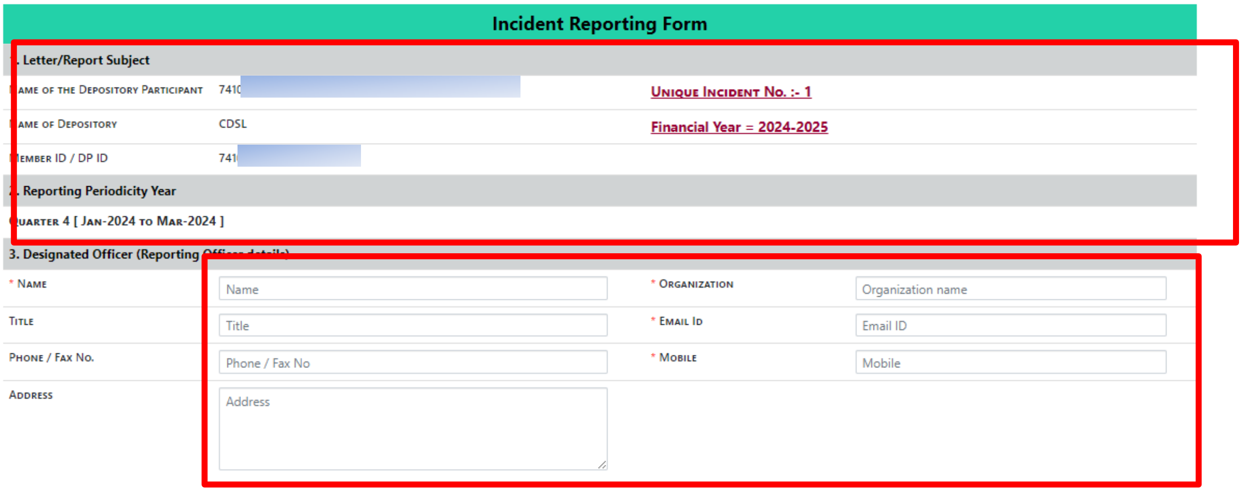
AUDIT APPLICATION

CYBER INCIDENT REPORT

Audit Type	CYBER INCIDENT REPORT	DP Name(ID)	74[redacted] LI
Audit Month	202403	Period	Jan-2024 to Mar-2024
DP ID	74[redacted]		

Cyber Incident Report covers the following Branch DPIDs :-

6. Fill in the details in the prescribed format in:
    1. **Letter/Report Subject**
    2. **Reporting Periodicity Year**
    3. **Designated Officers details**.



Incident Reporting Form

. Letter/Report Subject

ame of the Depository Participant	741[redacted]	Unique Incident No. :- 1
ame of Depository	CDSL	Financial Year = 2024-2025
ember ID / DP ID	741[redacted]	

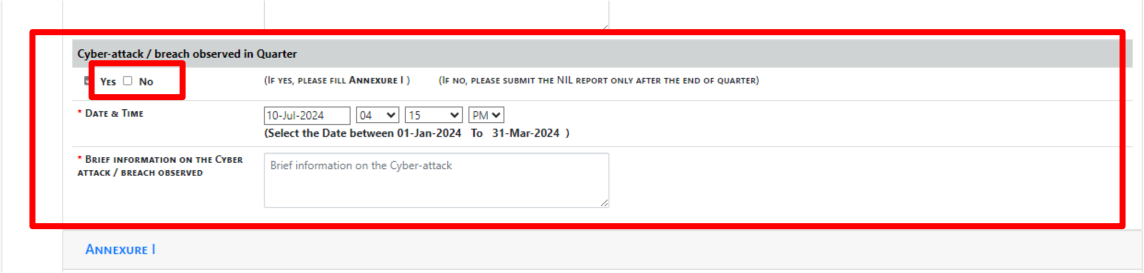
. Reporting Periodicity Year

uarter 4 [Jan-2024 to Mar-2024]

3. Designated Officer (Reporting Officer details)

* Name	Name	* Organization	Organization name
Title	Title	* Email Id	Email ID
Phone / Fax No.	Phone / Fax No	* Mobile	Mobile
Address	Address		

7. Select the option **Yes** in Cyber-attack/breach observed in Quarter and fill the below required information:
    - Date & Time
    - Brief information on the Cyber attack
    - Then Click on Annexure I



Cyber-attack / breach observed in Quarter

☑ Yes ☐ No (If yes, please fill Annexure I) (If no, please submit the NIL report only after the end of quarter)

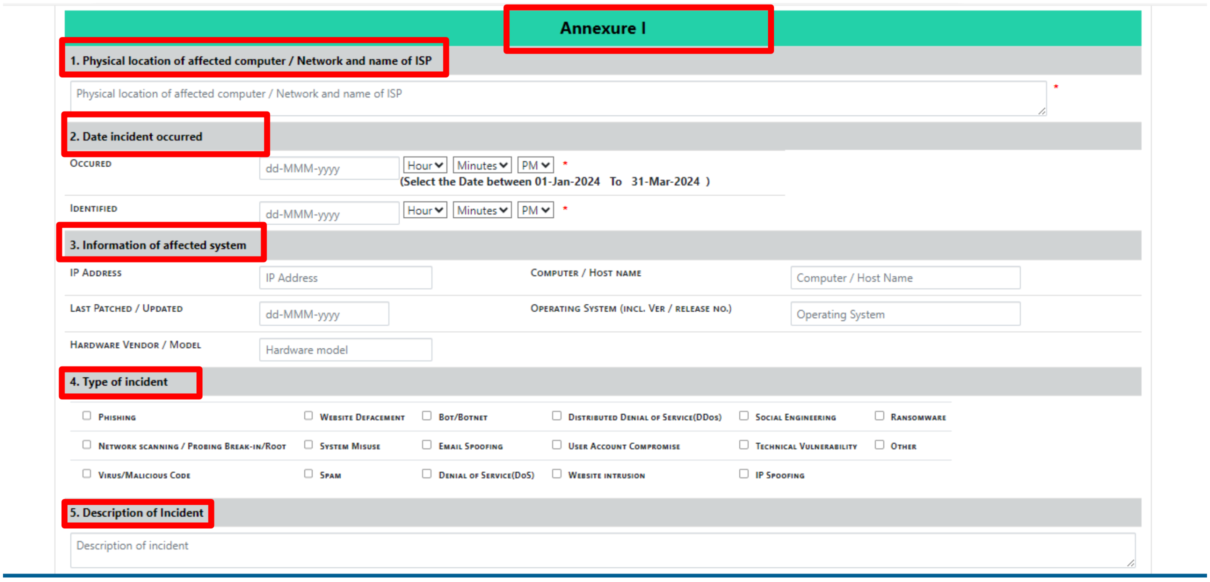
* Date & Time 10-Jul-2024 04 15 PM
(Select the Date between 01-Jan-2024 To 31-Mar-2024)

* Brief information on the Cyber attack / breach observed: Brief information on the Cyber-attack

Annexure I

8. Fill the relevant details in **Annexure I**:

1. Physical location of affected computer/ Network and name of ISP
2. Date incident occurred
3. Information of affected system
4. Select the type/types of incidents
5. Description of incident



Annexure I

1. Physical location of affected computer / Network and name of ISP

Physical location of affected computer / Network and name of ISP *

2. Date incident occurred

Occured: dd-MMM-yyyy Hour Minutes PM *
(Select the Date between 01-Jan-2024 To 31-Mar-2024)

Identified: dd-MMM-yyyy Hour Minutes PM *

3. Information of affected system

IP Address: IP Address
Computer / Host name: Computer / Host Name
Last Patched / Updated: dd-MMM-yyyy
Operating System (incl. Ver / release no.): Operating System
Hardware Vendor / Model: Hardware model

4. Type of incident

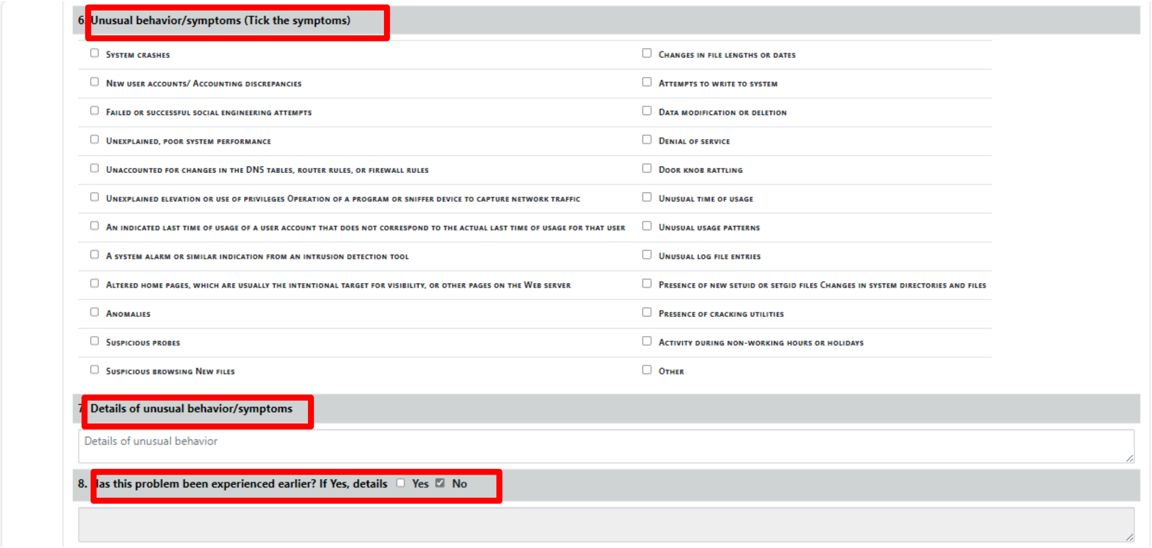
☐ Phishing ☐ Website Defacement ☐ Bot/Botnet ☐ Distributed Denial of Service(DDos) ☐ Social Engineering ☐ Ransomware
☐ Network scanning / Probing Break-in/Root ☐ System Misuse ☐ Email Spoofing ☐ User Account Compromise ☐ Technical Vulnerability ☐ Other
☐ Virus/Malicious Code ☐ Spam ☐ Denial of Service(DoS) ☐ Website intrusion ☐ IP Spoofing

5. Description of Incident

Description of incident

9. Fill the below Information:

- Select Unusual behaviour/symptoms (Tick the symptoms)
- Fill the Details of unusual behaviour/symptoms
- Has this problem been experienced earlier? If Yes, Give the description



6. Unusual behavior/symptoms (Tick the symptoms)

□ System crashes
□ New user accounts/ Accounting discrepancies
□ Failed or successful social engineering attempts
□ Unexplained, poor system performance
□ Unaccounted for changes in the DNS tables, router rules, or firewall rules
□ Unexplained elevation or use of privileges Operation of a program or sniffer device to capture network traffic
□ An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user
□ A system alarm or similar indication from an intrusion detection tool
□ Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server
□ Anomalies
□ Suspicious probes
□ Suspicious browsing New files

□ Changes in file lengths or dates
□ Attempts to write to system
□ Data modification or deletion
□ Denial of service
□ Door knob rattling
□ Unusual time of usage
□ Unusual usage patterns
□ Unusual log file entries
□ Presence of new setuid or setgid files Changes in system directories and files
□ Presence of cracking utilities
□ Activity during non-working hours or holidays
□ Other

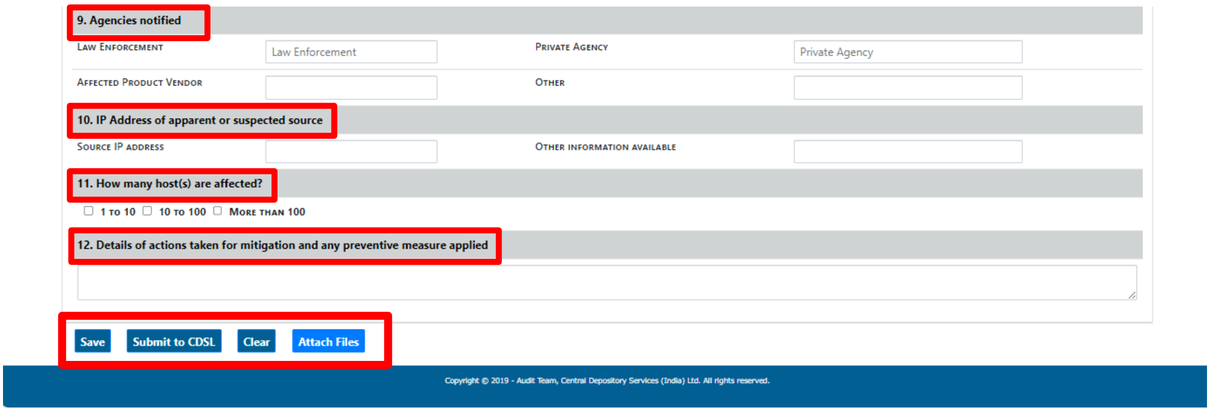
7. Details of unusual behavior/symptoms

Details of unusual behavior

8. Has this problem been experienced earlier? If Yes, details □ Yes ☑ No

10. Fill the below Information:

- Agencies notified
- IP Address of apparent or suspected source
- How many host(s) are affected?



9. Agencies notified

Law Enforcement	Law Enforcement	Private Agency	Private Agency
Affected Product Vendor		Other	

10. IP Address of apparent or suspected source

Source IP address		Other information available	

11. How many host(s) are affected?

□ 1 to 10 □ 10 to 100 □ More than 100

12. Details of actions taken for mitigation and any preventive measure applied

DPs can also save the multiple incidents in quarterly incident report module in audit web portal. After reporting each incident, please enter the "Save" **button & add another incident if any. After entering all the incidents, please enter the Submit to CDSL.**

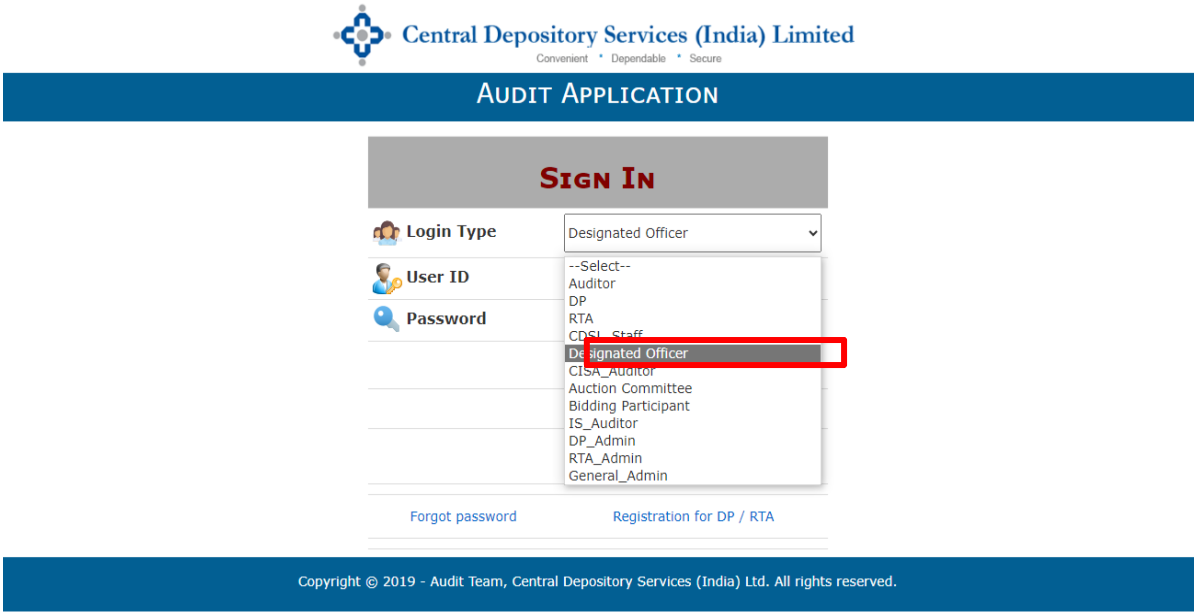
Attach Files: Click "**Attach Files**" to upload relevant documents.
Save: Click "Save" to save your information as a draft.
Submit to CDSL: Click "**Submit to CDSL**" to officially submit your report.
Clear: Click "**Clear**" to remove all entered data and reset the form.

***

Annexure B

Guidelines to submit Quarterly Cyber Incident Report

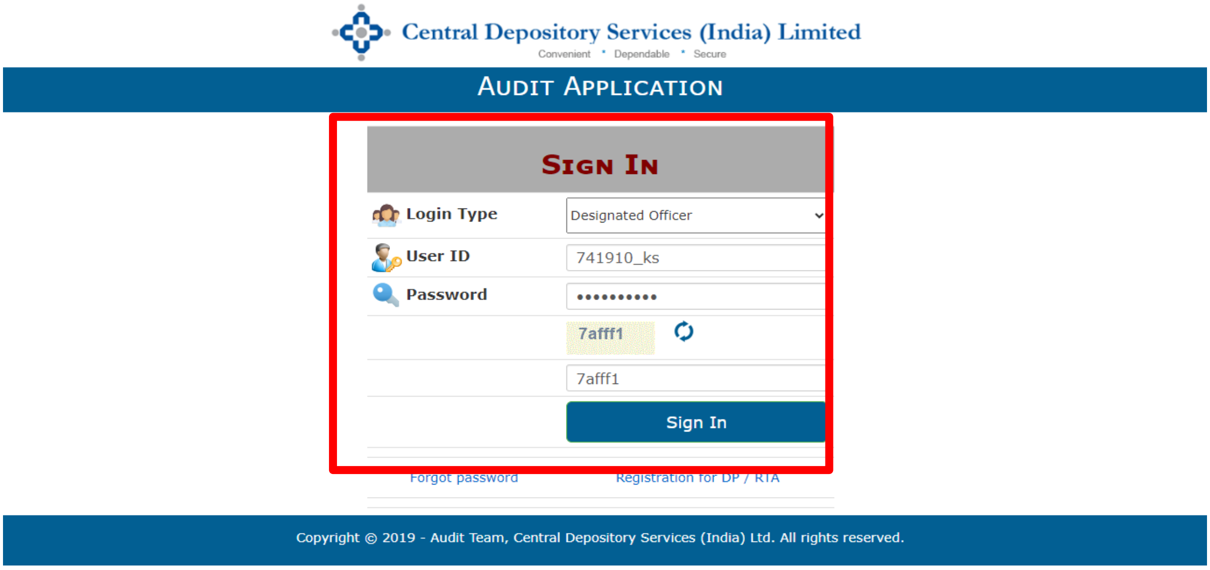
1. Open the Audit Web Portal.
    - Link: https://auditweb.cdslindia.com/Login.aspx
    - Click on Login Type and select "**Designated Officer**" login.



Login Type: Designated Officer

Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.

2. Fill the below required information and click on "**Sign In**" Button:
    - User ID, Password & Captcha



Central Depository Services (India) Limited
Convenient • Dependable • Secure
AUDIT APPLICATION
SIGN IN
Sign In
Forgot password
Registration for DP / RTA

Login Type: Designated Officer

User ID: 741910_ks

Password: ••••••••••

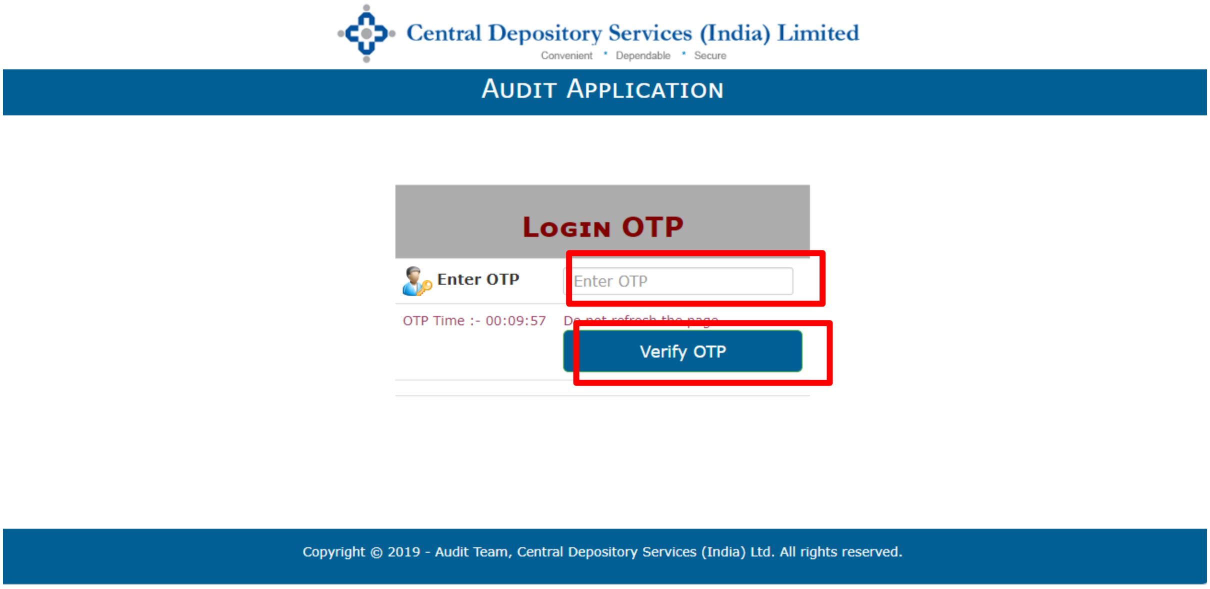
7afff1

7afff1

Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.

3. Enter the OTP:

- You will receive the OTP on both your DP's registered mobile number and email Id.



Central Depository Services (India) Limited

Convenient • Dependable • Secure

AUDIT APPLICATION

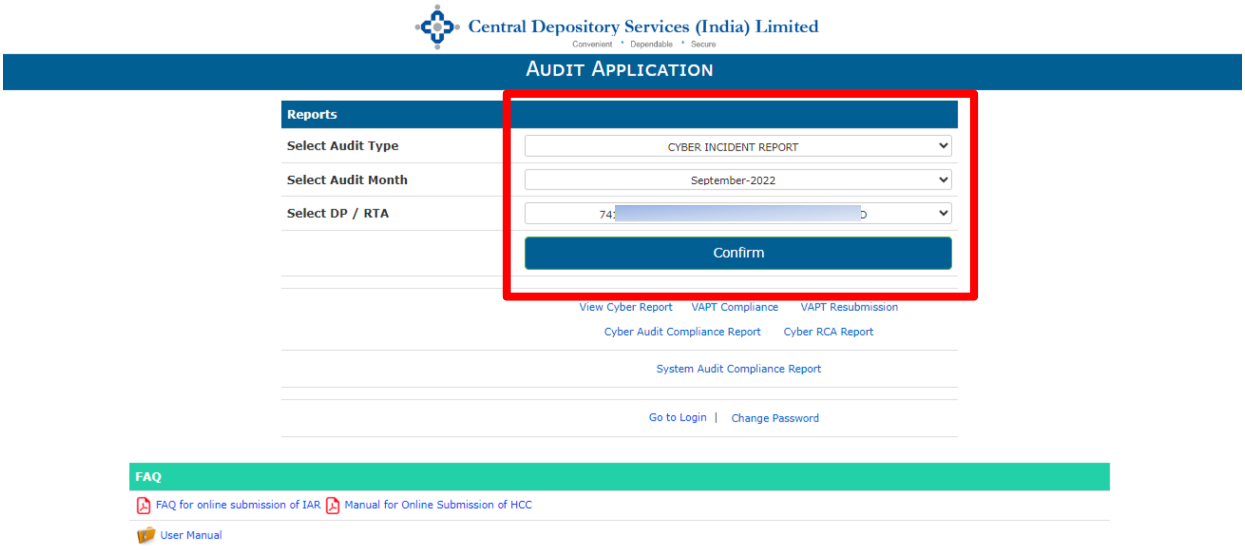
LOGIN OTP

Enter OTP	Enter OTP
OTP Time :- 00:09:57	Do not refresh the page

Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.

4. Select required information for submitting **quarterly** "**Cyber Incident**" report:

- Select Audit Type: **CYBER INCIDENT REPORT**
- Select Audit Month: **Select quarter month**
- Select DP/RTA: **Select your DP ID**
- Click on the "**Confirm**" Button



Central Depository Services (India) Limited

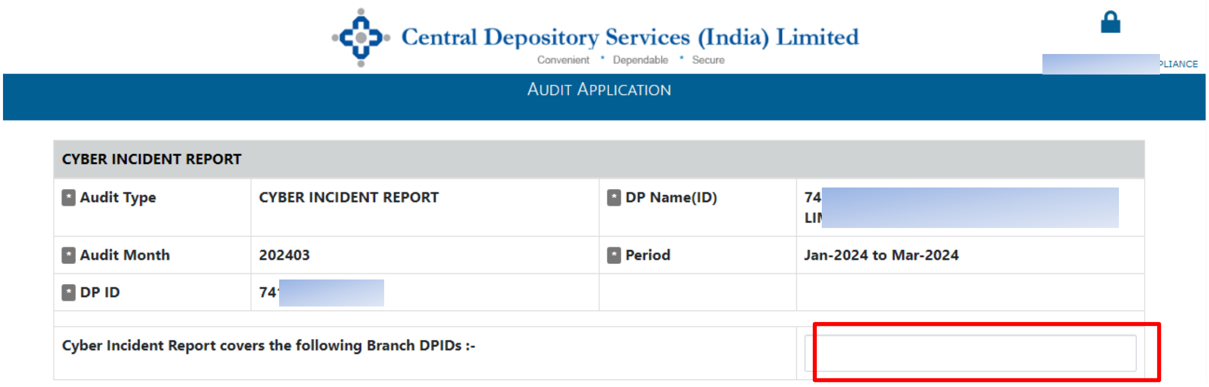
Convenient • Dependable • Secure

AUDIT APPLICATION

Reports	
Select Audit Type	CYBER INCIDENT REPORT
Select Audit Month	September-2022
Select DP / RTA	741[redacted]D

Confirm
View Cyber Report
VAPT Compliance
VAPT Resubmission
Cyber Audit Compliance Report
Cyber RCA Report
System Audit Compliance Report
Go to Login |
Change Password
FAQ
FAQ for online submission of IAR
Manual for Online Submission of HCC
User Manual

5. The following screen will appear. Main DP can mention the branch DP IDs , if they are submitting consolidated report for branch DP IDs.



Central Depository Services (India) Limited

Convenient • Dependable • Secure

[redacted]PLIANCE

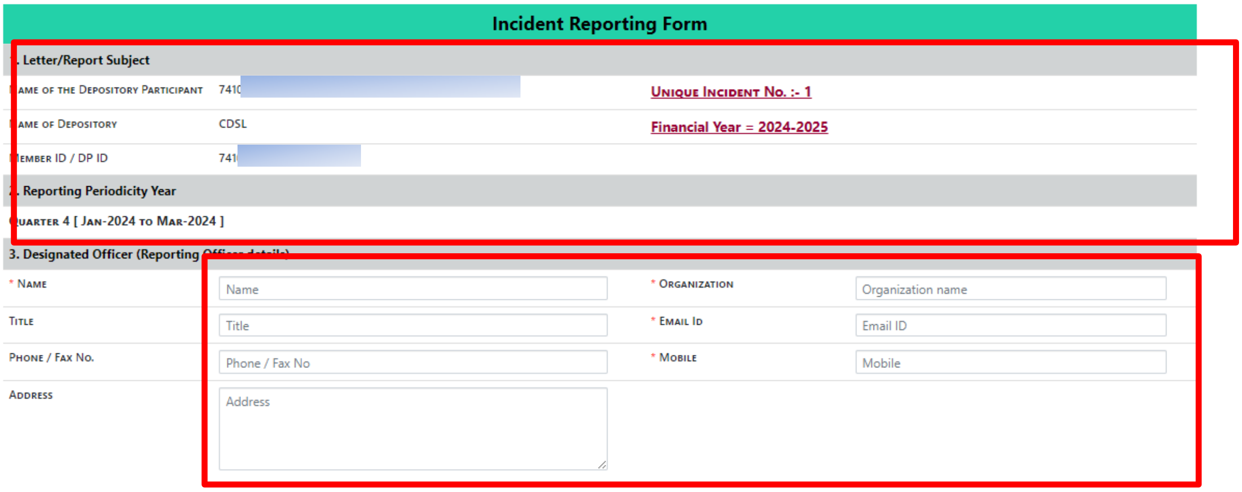
AUDIT APPLICATION

CYBER INCIDENT REPORT			
▪ Audit Type	CYBER INCIDENT REPORT	▪ DP Name(ID)	74[redacted] LI
▪ Audit Month	202403	▪ Period	Jan-2024 to Mar-2024
▪ DP ID	74[redacted]		

Cyber Incident Report covers the following Branch DPIDs :-

6. Fill in the details in the prescribed format in:

1. **Letter/Report Subject**
2. **Reporting Periodicity Year**
3. **Designated Officers details**.



Incident Reporting Form

1. Letter/Report Subject

Name of the Depository Participant	741[redacted]	Unique Incident No. :- 1	
Name of Depository	CDSL	Financial Year = 2024-2025	
Member ID / DP ID	741[redacted]		

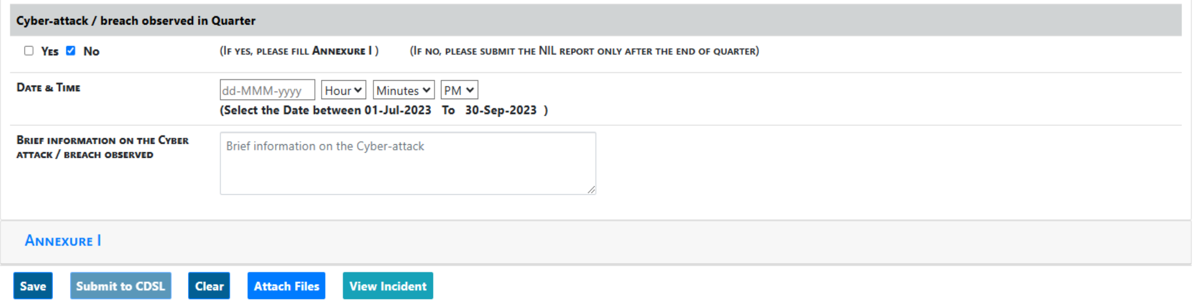
2. Reporting Periodicity Year

Quarter 4 [Jan-2024 to Mar-2024]

3. Designated Officer (Reporting Officer details)

* Name	Name	* Organization	Organization name
Title	Title	* Email Id	Email ID
Phone / Fax No.	Phone / Fax No	* Mobile	Mobile
Address	Address		

7. Select the option **NO** in Cyber-attack/breach observed in Quarter: **(If no incident has occurred)**



Cyber-attack / breach observed in Quarter

□ Yes ☑ No (If yes, please fill Annexure I) (If no, please submit the NIL report only after the end of quarter)

Date & Time: dd-MMM-yyyy | Hour | Minutes | PM
(Select the Date between 01-Jul-2023 To 30-Sep-2023)

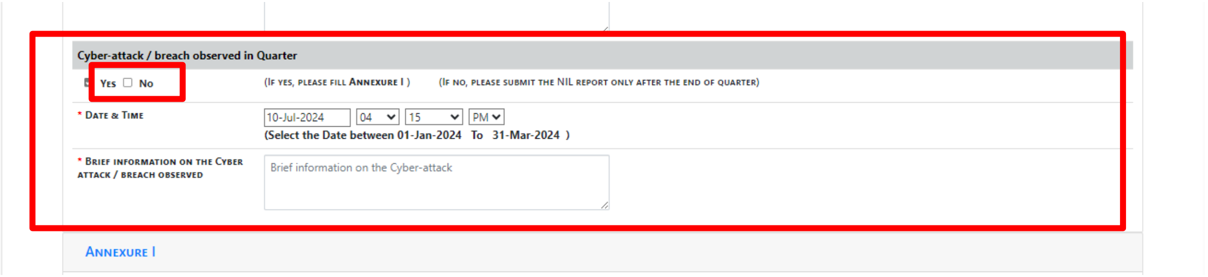
Brief information on the Cyber attack / breach observed: Brief information on the Cyber-attack

Annexure I

The Report is submitted as NIL report.

8. Select the option **Yes** in Cyber-attack/breach observed in Quarter and fill the below required information: **(if the incident occurred)**

- Date & Time
- Brief information on the Cyber attack
- Then Click on Annexure I



Cyber-attack / breach observed in Quarter

☑ Yes □ No (If yes, please fill Annexure I) (If no, please submit the NIL report only after the end of quarter)

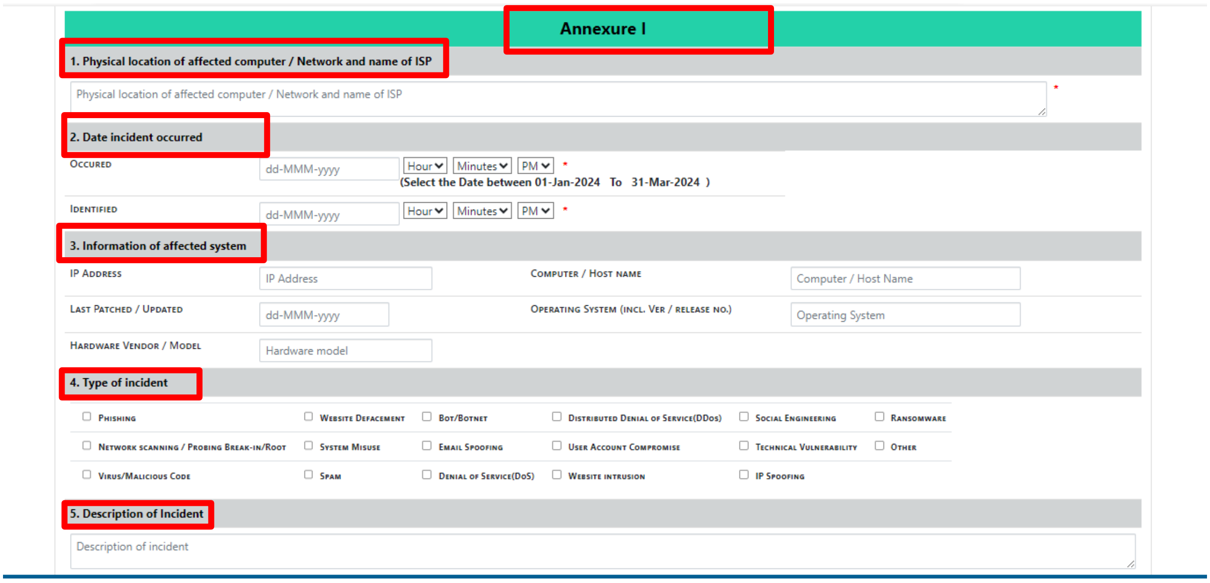
* Date & Time: 10-Jul-2024 | 04 | 15 | PM
(Select the Date between 01-Jan-2024 To 31-Mar-2024)

* Brief information on the Cyber attack / breach observed: Brief information on the Cyber-attack

Annexure I

9. Fill the **Annexure I**:

6. Physical location of affected computer/ Network and name of ISP
7. Date incident occurred
8. Information of affected system
9. Select the type/types of incidents
10. Description of incident



Annexure I

1. Physical location of affected computer / Network and name of ISP

Physical location of affected computer / Network and name of ISP *

2. Date incident occurred

Occured	dd-MMM-yyyy	Hour	Minutes	PM	*
	(Select the Date between 01-Jan-2024 To 31-Mar-2024)				
Identified	dd-MMM-yyyy	Hour	Minutes	PM	*

3. Information of affected system

IP Address	IP Address	Computer / Host name	Computer / Host Name
Last Patched / Updated	dd-MMM-yyyy	Operating System (incl. Ver / release no.)	Operating System
Hardware Vendor / Model	Hardware model		

4. Type of incident

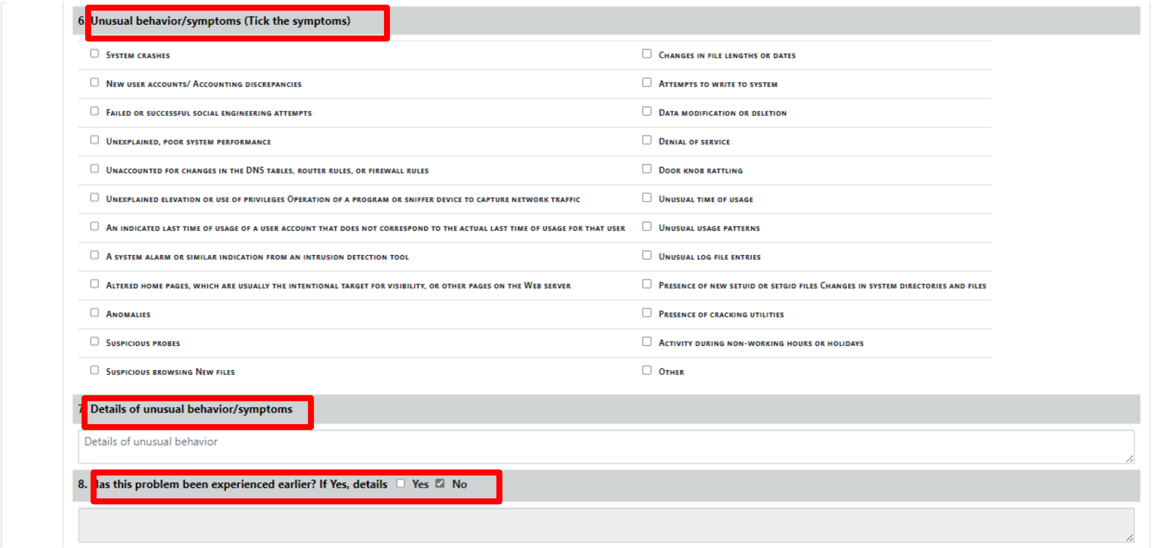
☐ Phishing	☐ Website Defacement	☐ Bot/Botnet	☐ Distributed Denial of Service(DDos)	☐ Social Engineering	☐ Ransomware
☐ Network scanning / Probing Break-in/Root	☐ System Misuse	☐ Email Spoofing	☐ User Account Compromise	☐ Technical Vulnerability	☐ Other
☐ Virus/Malicious Code	☐ Spam	☐ Denial of Service(DoS)	☐ Website intrusion	☐ IP Spoofing	

5. Description of Incident

Description of incident

10. Fill the below Information:

- Select Unusual behaviour/symptoms (Tick the symptoms)
- Fill the Details of unusual behaviour/symptoms
- Has this problem been experienced earlier? If Yes, Give the description



6. Unusual behavior/symptoms (Tick the symptoms)

☐ System crashes	☐ Changes in file lengths or dates
☐ New user accounts/ Accounting discrepancies	☐ Attempts to write to system
☐ Failed or successful social engineering attempts	☐ Data modification or deletion
☐ Unexplained, poor system performance	☐ Denial of service
☐ Unaccounted for changes in the DNS tables, router rules, or firewall rules	☐ Door knob rattling
☐ Unexplained elevation or use of privileges Operation of a program or sniffer device to capture network traffic	☐ Unusual time of usage
☐ An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user	☐ Unusual usage patterns
☐ A system alarm or similar indication from an intrusion detection tool	☐ Unusual log file entries
☐ Altered home pages, which are usually the intentional target for visibility, or other pages on the Web server	☐ Presence of new setuid or setgid files Changes in system directories and files
☐ Anomalies	☐ Presence of cracking utilities
☐ Suspicious probes	☐ Activity during non-working hours or holidays
☐ Suspicious browsing New files	☐ Other

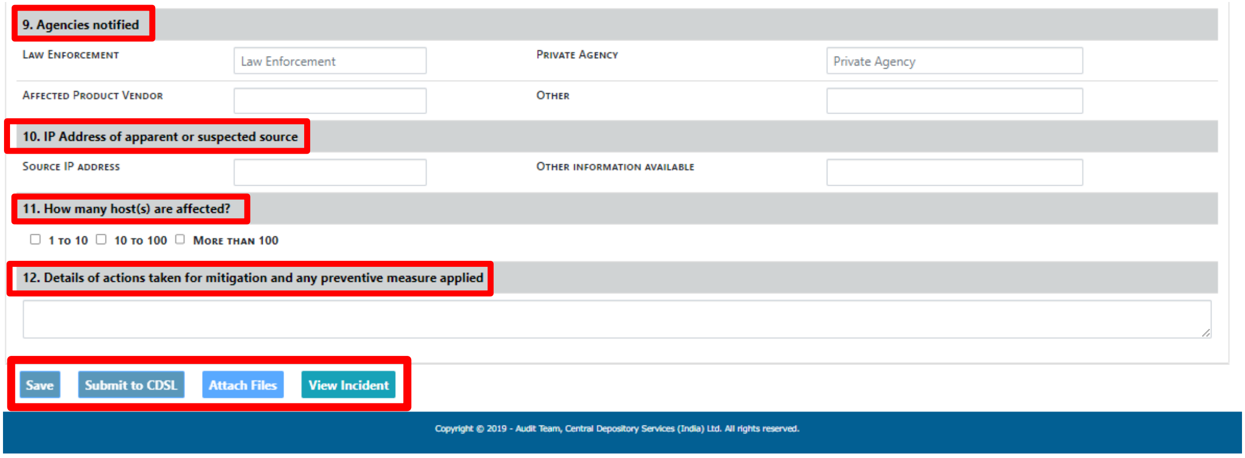
7. Details of unusual behavior/symptoms

Details of unusual behavior

8. las this problem been experienced earlier? If Yes, details ☐ Yes ☑ No

11. Fill the below Information:

- Agencies notified
- IP Address of apparent or suspected source
- How many host(s) are affected?



9. Agencies notified

Law Enforcement	Law Enforcement	Private Agency	Private Agency
Affected Product Vendor		Other	

10. IP Address of apparent or suspected source

Source IP address		Other information available	

11. How many host(s) are affected?

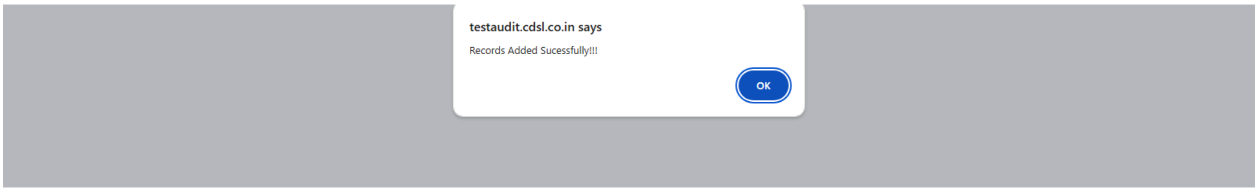
□ 1 to 10 □ 10 to 100 □ More than 100

12. Details of actions taken for mitigation and any preventive measure applied

Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.

Attach Files: Click "**Attach Files**" to upload relevant documents.

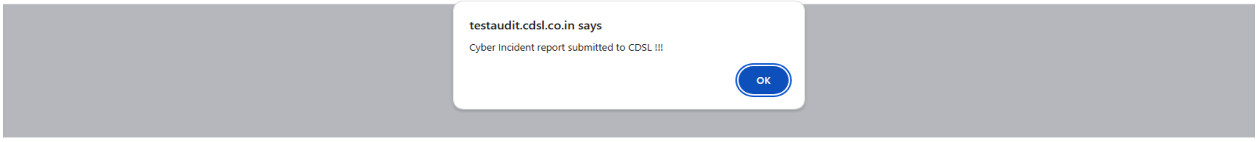
Save: Click "Save" to save your information as a draft.



testaudit.cdsl.co.in says

Records Added Sucessfully!!!

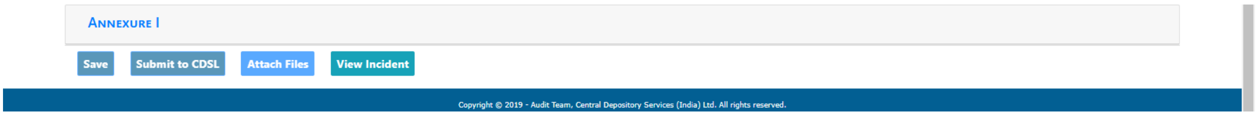
Submit to CDSL: Click "**Submit to CDSL**" to officially submit your report.



testaudit.cdsl.co.in says

Cyber Incident report submitted to CDSL !!!

View Incident: Click “**View Incident**” to see your submitted reports history.



Annexure I

Copyright © 2019 - Audit Team, Central Depository Services (India) Ltd. All rights reserved.

Note:

- **All incidents report activities must be completed in one continuous action, from saving to submitting the incident sreport.**
- **Once you submit the incident report, it cannot be submitted again.**
- **When you re-login, the scheduled month/DP ID will not appear, that means you have already submitted the incident report.**

***